I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Predictive Surveillance and the Threat to Fourth Amendment Jurisprudence

SHAUN B. SPENCER*

CONTENTS

* Assistant Professor and Director of Legal Skills, University of Massachusetts School of Law-Dartmouth.

This Article explores how the use of predictive surveillance to prevent terrorist and criminal activity may shape Fourth Amendment law. Predictive surveillance refers to a potential model of surveillance in which government collects data in bulk and then uses predictive analytics to detect patterns indicating terrorist or criminal activity. The existing model of surveillance regulation presumes that the government's first step is to target a specific person. Therefore, the first analytical step in evaluating the constitutionality of a given surveillance practice is to determine whether the government had sufficient particularized suspicion about the target. Predictive surveillance, however, confounds the existing model because it requires collection of massive amounts of data with no particularized suspicion. Despite that disconnect, judges will face great pressure to twist existing doctrine rather than ban the data collection that the government claims is necessary to fight terrorism or crime. Assuming that courts will be predisposed to find predictive surveillance constitutional, this Article explores the various doctrinal approaches that courts could take to approve predictive surveillance and assesses the risk that each approach poses to Fourth Amendment doctrine.[1]

Part I introduces the concept of predictive analytics and describes predictive surveillance as a potential application of predictive analytics. Part II first identifies the technical and political challenges that the government will face if it tries to implement predictive surveillance and then discusses the reasons to believe that researchers and political actors will overcome these challenges. Part III describes why predictive surveillance threatens Fourth Amendment doctrine itself and offers a cautionary tale of how courts evaluating a prior mass surveillance program twisted the statutory language to authorize the program. Part IV discusses the different ways that courts could apply the Fourth Amendment's third-party and public-exposure doctrines to predictive surveillance and then assesses how each approach could affect the development of those doctrines. Finally, Part V discusses the different

[1] This Article focuses on the constitutionality of the data collection necessary to conduct predictive surveillance. This Article does not address the constitutionality of using predictive analytics on data that the government already possesses or that third parties have sold to the government or shared with the government voluntarily.

ways that courts could apply the Fourth Amendment reasonableness standard to predictive surveillance and assesses how each approach could affect the reasonableness standard.

I. WHAT IS PREDICTIVE SURVEILLANCE?

Predictive surveillance is one potential application of predictive analytics, a branch of data science that predicts future behavior based on the patterns found in past behavior.[2] Predictive analytics applies statistical and computational tools to often massive volumes of data to find and act upon patterns in the data. One common approach to predictive analytics involves "training" a predictive algorithm on a subset of data about which you know the outcome, testing the algorithm on a different subset of that data, and finally applying the algorithm in real time to emerging data to help predict future outcomes.[3]

Public and private entities alike are using predictive analytics. Employers analyze employee data to predict which employees are likely to leave and decide how to retain employees at risk of departure.[4] Merchants use predictive analytics to identify customers likely to switch to competing products or services.[5] Manufacturers use real-time data from "smart" devices to predict when machines will fail.[6] Doctors use patient data to build algorithms to predict which intensive care unit patients will develop sepsis.[7] Government agencies use predictive

---

[2] ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 11, 80 (2013).

[3] VIJAY KOTU & BALA DESHPANDE, PREDICTIVE ANALYTICS AND DATA MINING: CONCEPTS & PRACTICE WITH RAPIDMINER 17-19, 27-28 (2015).

[4] John Boudreau, *Predict What Employees Will Do Without Freaking Them Out*, HARV. BUS. REV. (Sept. 5, 2014), https://hbr.org/2014/09/predict-what-employees-will-do-without-freaking-them-out [https://perma.cc/69TH-SU7G].

[5] *Analyzing Customer Churn by Using Azure Machine Learning*, MICROSOFT AZURE (Dec. 13, 2016), https://docs.microsoft.com/en-us/azure/machine-learning/machine-learning-azure-ml-customer-churn-scenario [https://perma.cc/68R5-CLM3].

[6] Jacob LaRiviere et al., *Where Predictive Analytics Is Having the Biggest Impact*, HARV. BUS. REV. (May 25, 2016), https://hbr.org/2016/05/where-predictive-analytics-is-having-the-biggest-impact [https://perma.cc/38GV-UYGA].

[7] Thomas Desautels et al., *Prediction of Sepsis in the Intensive Care Unit with Minimal Electronic Health Record Data: A Machine Learning Approach*, JMIR MED. INFORM. (Sept. 30, 2016),

analytics to identify fraud in tax returns and government contracts.[8] Predictive analytics is already in widespread private and public sector use, and its footprint is growing.[9]

Predictive surveillance refers to the potential use of predictive analytics to predict terrorist or criminal activity.[10] As with any use of predictive analytics, predictive surveillance requires massive data collection in order to build and test predictive models and then apply those models in real time.

Predictive surveillance differs from traditional surveillance because traditional surveillance begins with a targeting decision. Under the traditional surveillance model, the government first decides to target someone based on some degree of particularized suspicion.[11] Under predictive surveillance, however, the government would not begin with any degree of individualized suspicion about a surveillance target. In

---

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5065680/?report=printable [https://perma.cc/YCN6-ZSDU].

[8] SIEGEL, *supra* note 2, at tbl.5; *Government: Our Work*, ELDER RESEARCH, INC., http://dataminginglab.com/solutions/industries/government [https://perma.cc/LA3C-4FB2].

[9] *See, e.g.*, Louis Columbus, *89% of B2B Marketers Have Predictive Analytics On Their Roadmaps For 2016*, FORBES (Jan. 24, 2016), https://www.forbes.com/sites/louiscolumbus/2016/01/24/89-of-b2b-marketers-have-predictive-analytics-on-their-roadmaps-for-2016/#52efdcbf1822 [https://perma.cc/ML7Z-CM8L] (reporting survey findings that 49 percent of business to business marketers already use predictive analytics, and 40 percent plan to start using it within six months); LaRiviere et al., *supra* note 6 (discussing impact of predictive analytics for predicting consumer demand, optimizing consumer pricing, and predicting supply chain maintenance needs).

[10] Shaun B. Spencer, *When Targeting Becomes Secondary: A Framework for Regulating Predictive Surveillance in Anti-Terror Investigations*, 92 DENV. U. L. REV. 493, 495-96 (2015).

[11] *See, e.g.*, 18 U.S.C. § 2518(3)(a)–(b) (2012) (criminal investigators relying on the Wiretap Act must demonstrate to a court that there is probable cause to believe that the interception will reveal evidence of a felony listed in Section 2516); 18 U.S.C. § 2703(d) (2012) (under the Stored Communications Act, the government may compel an internet service provider to produce subscriber information by showing "reasonable grounds to believe" that the records are relevant and material to an ongoing criminal investigation); 50 U.S.C. § 1804(a)(3)(A) (2012) (foreign intelligence investigators seeking to intercept electronic communications under the Foreign Intelligence Surveillance Act must show probable cause to believe that the surveillance target is "a foreign power or an agent of a foreign power"); United States v. Jones, 565 U.S. 400, 404 (2012) (criminal investigators installing a GPS device to track a suspect's car must first obtain a warrant based on probable cause to believe that the tracking will reveal evidence of a crime).

fact, the government would have no target in mind at all. Instead, the government would begin by collecting and analyzing all available data to find patterns that correlate with past terrorist or criminal activity. Then the government would use predictive algorithms to identify similar patterns in emerging data and, based on those patterns, use traditional targeted surveillance to investigate the suspects.[12]

The constitutionality of predictive surveillance is a moot point unless the government actually attempts to implement it. The next Part, therefore, discusses the extent to which predictive surveillance is technically and politically possible.

II. THE TECHNICAL AND POLITICAL FEASIBILITY OF PREDICTIVE SURVEILLANCE

If predictive surveillance never becomes technically or politically viable, then courts will not have to confront the constitutional issues discussed below. This Part first discusses the technical challenges to predictive surveillance and the reasons to believe that researchers will overcome those challenges. This Part next discusses the historical public opposition to pervasive surveillance technologies and the reasons to believe that the government will nevertheless implement predictive surveillance if it becomes technically viable.

A. *The Potential of Predictive Surveillance as a Counter-Terrorism and Law Enforcement Tool*

Predicting terrorist activity is an especially challenging application of predictive analytics for several reasons. First, terrorist activity has a very low "base rate" because it occurs quite rarely.[13] Some experts have argued that terrorist attacks and plots are so rare that they will not generate a unique signature that can be heard above the noise of all

---

[12] Spencer, *supra* note 10, at 504.

[13] Neil D. Shortland, *"On the Internet, Nobody Knows You're a Dog": The Online Risk Assessment of Violent Extremists, in* COMBATING VIOLENT EXTREMISM & RADICALIZATION IN THE DIGITAL ERA 352 (Majeed Khader et al. eds., 2016) ("COMBATING VIOLENT EXTREMISM"); Jenna McLaughlin, *The White House Asked Social Media Companies to Look for Terrorists. Here's Why They'd #Fail*, THE INTERCEPT, (Jan. 20, 2016), https://theintercept.com/2016/01/20/the-white-house-asked-social-media-companies-to-look-for-terrorists-heres-why-theyd-fail/ [https://perma.cc/76Z8-RPPB].

online activity.[14] Second, given the vast amount of internet activity, using predictive analytics may produce many "false positives."[15] Predictive surveillance is vulnerable to false positives because it may be difficult to discern patterns that distinguish terrorism-related activity from innocent Internet activity.[16] Too many false positives will yield far too many suspects for law enforcement or counter-terrorism agents to pursue.

However, there is reason to believe that researchers may overcome these technical obstacles. First, with regard to low base rates, the unfortunate reality is that terrorist plots and attacks are becoming more common in the United States and across the globe. One source of data collection on domestic terrorism is the Empirical Assessment of Domestic Radicalization (EADR), a project of the National Consortium for the Study of Terrorism and Responses to Terrorism. EADR researchers built a dataset on individual radicalization in the United States from 1948 to 2013.[17] Their dataset includes several measures showing domestic terrorist activity on the rise since 2000. One measure tracks the numbers of individuals revealed to have been "radicalized."[18]

---

[14] Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, CATO INST. POLICY ANALYSIS 584, 7-8 (Dec. 11, 2006), http://object.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf [https://perma.cc/BLN5-7UQ5]; McLaughlin, *supra* note 13; Bruce Schneier, *Data Mining for Terrorists*, SCHNEIER ON SECURITY (Mar. 9, 2006), https://www.schneier.com/blog/archives/2006/03/data_mining_for.html [https://perma.cc/8QUD-MQPQ].

[15] Jonas & Harper, *supra* note 14, at 7-8; McLaughlin, *supra* note 13; Schneier, *supra* note 14.

[16] Jonas & Harper, *supra* note 14, at 8; David Romyn & Mark Kebbell, *Using the Internet to Plan for Terrorist Attack*, *in* COMBATING VIOLENT EXTREMISM, *supra* note 13, at 100; Shortland, *supra* note 13, at 352 (noting that extremists' online activities may be clear indicators of intent in hindsight, but finding those indicators in real time may be impossible because of how many other individuals demonstrate the same behavioral indicators online but lack the intent or capacity to take violent action).

[17] *Empirical Assessment of Domestic Radicalization (EADR)*, NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM, http://www.start.umd.edu/research-projects/empirical-assessment-domestic-radicalization-eadr [https://perma.cc/QK9K-G93C].

[18] Though the term "radicalized" may be susceptible of conflicting and controversial interpretations, the EADR study defines it quite broadly. The EADR dataset includes "individuals espousing Islamist, far right, far left, or single-issue ideologies who have radicalized within the United States to the point of committing ideologically motivated illegal violent or non-violent acts, joining a terrorist organization, or associating with an extremist organization whose leader(s) has/have been indicted of an ideologically

The EADR dataset shows that the number of individuals revealed as radicalized stood at 193 in the 1970s, 242 in the 1980s, and 298 in the 1990s. In the 2000s, however, that figure jumped to 451, and the figure is on pace to exceed 400 this decade.[19] Another EADR measure tracks the number of terrorist plots in which those radicalized individuals were involved, ranging from "nebulous" plots to executed attacks. There were 117 plots discovered in the 1970s, 148 in the 1980s, and 142 in the 1990s. In the 2000s, the total jumped to 209, and the figure is on pace to exceed 200 again in the 2010s.[20]

Second, with regard to a discernible terrorism "signature," terrorist activity increasingly occurs online. The Internet has become an important tool for violent extremist organizations.[21] It plays a central

---

motivated violent offense." NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM, PROFILES OF INDIVIDUAL RADICALIZATION IN THE UNITED STATES (PIRUS) CODEBOOK 3 (2016), http://www.start.umd.edu/sites/default/files/files/research/PIRUSCodebook.pdf [https://perma.cc/9P6E-PSSF]. More specifically, the EADR treats the following as "radicalized":

> anyone arrested, indicted, and/or convicted of either engaging or planning to engage in ideologically motivated unlawful behavior, or anyone who belonged to a designated terrorist organization or a violent extremist group. For planned violence, there must be a fairly direct connection between the individual and the plot. Note: radicalization does not necessarily involve violence. An individual who provides material support to an Islamist group because he/she identifies with the group's goals but does not participate in any attacks, or someone who runs a website for a violent extremist group, or is arrested for trespassing because they were stalking an individual for ideological reasons (like animal rights activists harassing employees of medical research labs) would count as radicalized. Note: radicalization does not include non-ideological criminal acts or legal ideological activities. For example, selling weapons to a group for material gains rather than ideological affinity would not count as radicalized. And someone who openly supports an extremist group that participates in politics (such as voting for a Communist Party candidate for office) would also not be radicalized.

Id. at 4-5.

[19] *Empirical Assessment of Domestic Radicalization (EADR)*, NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM, http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus [https://perma.cc/3AU3-LC5A].

[20] *Id.*

[21] Fredrik Johansson et al., *Detecting Linguistic Markers of Violent Extremism in Online Environments*, *in* COMBATING VIOLENT EXTREMISM, *supra* note 13, at 375; Jennifer Yang Hui, *Social Media Analytics for Intelligence and Countering Violent Extremism*, *in* COMBATING VIOLENT EXTREMISM, *supra* note 13, at 328; Robyn Torok, *Social Media and the Use of Discursive Markers of Online Extremism & Recruitment*, *in* COMBATING

role in recruitment, planning, and operations by foreign insurgencies on United States soil.[22] Similarly, according to the United Kingdom's domestic security agency, MI5, at least seven of the last ten attacks in the United Kingdom since 2010 involved perpetrators who read Al-Quaeda's online platform *Inspire*, which "significantly enhanced" the capacity of four of those ten perpetrators.[23] Extremist organizations use the Internet "to recruit, deliver threats, release instructional materials to facilitate the actions of others, and plan and coordinate violent extremist attacks."[24] Data from the Empirical Assessment of Domestic Radicalization[25] confirms that terrorist recruitment and planning in the United States increasingly involves the Internet. The EADR dataset shows that, for the 250 radicalized individuals involved in domestic terrorist plots revealed in the United States since 2005, the Internet played a primary role in the radicalization of 30 (12%), and played some role in the radicalization of an additional 92 (37%).[26] Of the 156 planned, failed, and successful domestic plots by those radicalized individuals, the Internet was used for communications or logistics in 68 of them (44%).[27]

Even lone wolf attackers have increasingly visible online profiles. Many lone wolf attackers "are only loners in their offline life, but are often very active in communicating their views and radical opinions in

---

VIOLENT EXTREMISM, *supra* note 13, at 39 ("Social media has now become the mainstream recruitment platform for online radicals and extremists.").

[22] Shortland, *supra* note 13, at 350.

[23] *Id.*

[24] *Id.* The Internet plays three main roles in radicalization: indoctrinating recruits into the organization's belief system, distributing the organization's ideology, and socializing recruits to provide them a sense of community. Erin Marie Saltman, *Western Female Migrands to ISIS: Propaganda, Radicalization, & Recruitment*, *in* COMBATING VIOLENT EXTREMISM, *supra* note 13, at 180.

[25] *See*, NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM, *supra* note 18; *see also*, *EADR*, *supra* note 19.

[26] Dataset available for download at: *Profiles of Individual Radicalization in the United States (PIRUS)*, NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM, http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus [https://perma.cc/Y776-MZCD].

[27] *Id.*

various discussion groups or other kinds of social media."[28] In fact, "[a]lmost all lone wolf attacks in recent years have involved the use of social media."[29] A study of 98 lone-actor terrorist plots in EU countries from 2000 to 2014 found that the perpetrators' social media use increased steadily since 2004.[30] One-third of those lone-actor terrorists used the Internet for tactical research such as downloading manuals, watching training videos, or basic reconnaissance.[31]

In addition to relying on the increased number and Internet visibility of terrorist plots, researchers can maximize their chances of detecting meaningful signals by training algorithms not on rare events like successful attacks, but on more common events like radicalization and nascent plots and on events involving networks that generate larger signals. Even if researchers are unable to produce algorithms identifying individuals with perfect accuracy, they may be able to flag a manageable number of potential suspects for human analysts to investigate further.[32] Additionally, predictive surveillance could prove successful in detecting activity with a higher base rate such as cyber-attacks, money laundering, or fraud.

Researchers are beginning to tackle these technical problems. For example, Johansson *et al.* developed a prototype for an online tool to detect warning behaviors predicting online violent extremism.[33] They focused on three warning behaviors most likely to appear in social

---

[28] Joel Brynielsson et al., *Harvesting and analysis of weak signals for detecting lone wolf terrorists*, SECURITY INFORMATICS (2013), https://security-informatics.springeropen.com/track/pdf/10.1186/2190-8532-2-11?site=security-informatics.springeropen.com [https://perma.cc/3WQC-DJ3F].

[29] Loo Seng Neo, *An Internet-Mediated Pathway for Online Radicalisation: RECRO, in* COMBATING VIOLENT EXTREMISM 199; Shortland, *supra* note 13, at 197-225.

[30] Clare Ellis et al., *Lone-Actor Terrorism*, ROYAL UNITED SERVS. INST. FOR DEF. & SEC. STUDIES, 5-6, 13 (2016), https://rusi.org/publication/occasional-papers/lone-actor-terrorism-analysis-paper [https://perma.cc/N78A-DEWC]. *Accord* Paul Gill et al., *Indicators of Lone Actor Violent Events: The Problems of Low Base Rates and Long Observational Periods*, 3(3-4) J. OF THREAT ASSESSMENT & MGMT., Vol. 3(3-4), 166, 169 (Sept. 2016). (finding that lone wolf actors from 2006 to 2013 were more likely to use the Internet in their attack planning than lone wolf actors from 1990 to 2005).

[31] Ellis, *supra* note 30, at 13.

[32] Brynielsson et al., *supra* note 28.

[33] Johansson et al., *supra* note 21, at 376.

media text: leakage, fixation, and identification.[34] The tool extracted relevant data from social media and used keywords and natural language processing to identify warning behaviors.[35] The researchers put the tool into operation by scanning the social media equivalent of several million documents a day for three days.[36] In that time, they received 130 hits for posts suggesting violent intent and making at least one favorable reference to bombs or weapons.[37]

Another recent study bridged the gap between using social media to predict civil unrest and studying online terrorist activity.[38] Johnson *et al.* used subject matter expertise and natural language processing to identify online pro-ISIS groups, or "aggregates."[39] Their primary conclusions related to development, disruption, and regeneration of aggregates.[40] However, their research also showed a connection between online aggregates and real-world events. They found that an escalation in pro-ISIS aggregates corresponded with the ISIS assaults on Kobani in September 2014.[41] In addition, their study suggested that, "instead of having to analyze the online activities of many millions of

---

[34] *Id.* at 377. The warning behaviors are drawn from a broader body of research studying predictors of targeted violence. *Id.* Leakage means "communication of intent to do harm to a third party." Fixation means behavior "which indicates an increasing pathological preoccupation with a person or cause." And identification means "a behavior which indicates a desire to be a 'pseudo-commando' – i.e., have a warrior mentality, closely associate with weapons or other military or law enforcement paraphernalia, identify with previous attackers or assassins, or identify oneself as an agent to advance a particular cause." *Id.*

[35] *Id.* at 378, 383-84.

[36] *Id.* at 385.

[37] *Id.* Deploying a tool like this would not be a self-effecting warning device. Instead, it would be used to flag high-risk individuals for review by human analysts. *Id.* at 378. Because this project was merely a prototype, the researchers did not attempt to investigate the 130 hits. They did add a filter for anti-Semitic sentiment which yielded four hits – a "Neoconservative Right magazine, a Christian blog, and two anti-Jewish blogs." *Id.* at 385. The researchers speculated that a real-world analyst who found these results would probably take no further action unless the websites had already been flagged. *Id.*

[38] N.F. Johnson et al., *New online ecology of adversarial aggregates: ISIS and beyond*, SCIENCE, June 2016, at 1459.

[39] *Id.* at 1460.

[40] *Id.* at 1462.

[41] *Id.* at 1461.

individual potential actors worldwide, interested parties can shift their focus to aggregates, of which there will typically be only a few hundred."[42] By suggesting both predictive value and a manageable dataset, this study offers some hope for predictive surveillance as a tool in the fight against terrorism.

In addition to using online behavior to predict real-world terrorist attacks, researchers may also use online behavior to predict cyber-attacks. One way to predict cyber-attacks is to study the online characteristics of websites that have and have not suffered attacks in the past. Researchers at Carnegie Mellon did just that when they trained a classification algorithm to predict which websites would be subject to cyber-attacks.[43] A second approach is to analyze the transactional data itself to identify patterns in the cyber-attacks. For example, MIT researchers developed a tool that predicts cyber-attacks by analyzing online transactions with potential cyber-attack targets.[44] A third approach significantly expands the types of data one might analyze to predict cyber-attacks. For example, the Intelligence Advanced Research Projects Activity runs a program called "CAUSE," which funds research on using "unconventional" signals to predict cyberattacks.[45] In one such project, researchers at the Rochester Institute of Technology developed a classifier to predict cyber-attacks based on references to the target company and to cyber-attacks in general on Twitter as well as in databases of world media coverage.[46]

---

[42] *Id.* at 1463.

[43] Patrick Howell O'Neill, *Carnegie Mellon researchers create Big Data tool to predict cyberattacks*, DAILY DOT (Aug. 21, 2014), https://www.dailydot.com/debug/website-hack-prediction-big-data-carnegie-mellon/ [https://perma.cc/27LY-Y5K4].

[44] Kalyan Veeramachaneni et al., *AI²: Training a Big Data Machine to Defend*, 2016 IEEE INT. CONF. BIGDATASECURITY, HPSC, & IDS 49-52 (2016) http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.79 [https://perma.cc/YVN4-RDZV].

[45] *Cyber-Attack Automated Unconventional Sensor Environment (CAUSE)*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, https://www.iarpa.gov/index.php/research-programs/cause/cause-baa [https://perma.cc/VN2Z-2CLY].

[46] AHMET OKUTAN ET AL., PREDICTING CYBER ATTACKS WITH BAYESIAN NETWORKS USING UNCONVENTIONAL SIGNALS §§ 1, 2.1, http://dx.doi.org/10.1145/3064814.3064823 [https://perma.cc/X9YT-3AFQ] (presented at Cyber and Information Security Research Conference 2017). The researchers gathered data on the total number and type of global cyberattacks each day from Hackmageddon.com, which provides global cyber-attack statistics. *Id.* The researchers also drew world events data from GDELT, the "Global Database of Events, Language, and Tone." *Id.* The GDELT Project "monitors the world's

Other CAUSE-funded research considers unconventional predictors such as black market prices for malware and internet search queries that may show attackers trying to map IP lists to plan their attack strategy.[47]

In sum, although predictive surveillance faces significant technical challenges, there is reason to believe that researchers will overcome them in at least some applications.

B. *The Political Viability of Predictive Surveillance as a Counter-Terrorism and Law Enforcement Tool*

Based on recent backlashes after secret surveillance programs came to light, predictive surveillance would face significant public resistance. In the wake of the September 11, 2001 terror attacks, public sentiment was as favorable as one could imagine toward government surveillance. The resulting shock and fear muted public opposition to the USA PATRIOT Act's expanded surveillance powers.[48] Yet just two years later, politicians and the public expressed outrage after learning of a research project within the Defense Advanced Research Projects Agency (DARPA) called "Total Information Awareness."[49] Total

---

broadcast, print, and web news from nearly every corner of every country in over 100 languages and identifies the people, locations, organizations, counts, themes, sources, emotions, counts, quotes, images and events driving our global society every second of every day, creating a free open platform for computing on the entire world." *Intro*, THE GDELT PROJECT, http://gdeltproject.org [https://perma.cc/SFS3-8KT8].

[47] Elisabeth Eaves, *IARPA Director Jason Matheny advances tech tools for US espionage*, 73 Bulletin of the Atomic Scientists no. 2, 2017, at 67, 72, http://dx.doi.org/10.1080/00963402.2017.1288430 [https://perma.cc/KSN3-Y3BS].

[48] Linda Greenhouse, *The Clamor of a Free People*, N.Y. TIMES, (Sept. 16, 2001), http://www.nytimes.com/2001/09/16/weekinreview/war-zone-what-price-liberty-the-clamor-of-a-free-people.html?mcubz=1 (observing that, after September 11, 2001, the balance between liberty and security "will now be recalibrated to reflect both new realities and new perceptions"); Calvin Woodward, *Muted after 9/11, NSA critics find their voice*, ASSOCIATED PRESS, (July 25, 2013,), http://www.sandiegouniontribune.com/sdut-muted-after-911-nsa-critics-find-their-voice-2013jul25-story.html [https://perma.cc/6Y77-45D4]; *Overwhelming Support for Bush, Military Response But...*, PEW RES. CTR. FOR THE PEOPLE & THE PRESS, (Sept. 19, 2001), http://www.people-press.org/2001/09/19/american-psyche-reeling-from-terror-attacks/ [https://perma.cc/29TC-8S52] (finding that most survey respondents believed the average person would have to give up some freedoms to prevent future terror attacks).

[49] BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 292 (2016); SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 230-48 (2010).

Information Awareness was the post-9/11 brainchild of John Poindexter, the former National Security Advisor under Ronald Regan who resigned after his role in the Iran-Contra Affair became public.[50] As Poindexter envisioned it, Total Information Awareness was an "early warning" surveillance system that would detect the digital signature that terrorists inevitably emitted in their purchases, phone calls, and travels.[51] The program operated out of the public spotlight as a DARPA research project.[52] When the program became public in 2003, scathing public criticism eventually led Congress to defund the program.[53] More recently, widespread public reaction to Edward Snowden's 2013 disclosure of the NSA's bulk telephone metadata collection program led Congress to pass the USA FREEDOM Act and end the bulk collection program.[54]

There are, however, reasons to believe that public opposition would not prevent the government from implementing a predictive surveillance program that promised to be an effective counter-terrorism or law enforcement tool. First, despite the public outcry, Congress did not completely kill the Total Information Awareness project. Although Congress formally defunded DARPA's Total Information Awareness project in a 2003 appropriations bill, Congress continued funding for significant Total Information Awareness programs in a "classified annex" to the bill – the so-called "black

---

[50] FRIEDMAN, *supra* note 49; HARRIS, *supra* note 49, at 65-66, 144-45.

[51] HARRIS, *supra* note 49, at 147; John Poindexter, *Overview of the Information Awareness Office*, FEDERATION OF AMERICAN SCIENTISTS (Aug. 2, 2002), https://fas.org/irp/agency/dod/poindexter.html [https://perma.cc/6BGP-M4QP]. *Accord* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 318 & n.6 (2008).

[52] GINA MARIE STEVENS, CONG. RESEARCH SERV., RL31730 PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS 1 (2003), https://fas.org/irp/crs/RL31730.pdf [https://perma.cc/HJN2-QA7U].

[53] FRIEDMAN, *supra* note 49; DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 183-84 (2016).

[54] LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 48-52 (2016).

budget."[55] Those programs moved out of DARPA to the National Security Agency's Advance Research and Development Activity.[56]

In addition, the federal government is sponsoring significant research efforts geared to predict both large-scale societal events like protests and small-scale events like terrorist activity. The Intelligence Advanced Research Projects Activity ("IARPA") is a research-funding entity within the Office of the Director of National Intelligence.[57] One major IARPA research initiative is "Anticipatory Intelligence," which "focuses on characterizing and reducing uncertainty by providing decision makers with timely and accurate forecasts of significant global events."[58]

Several active IARPA research programs are laying the groundwork for predictive surveillance, though they are not yet focused on predicting individual terrorist activity. The Mercury program is trying to develop "continuous, automated analysis of foreign [signals intelligence] data to anticipate and/or detect significant events, including military and terrorist activities, political crises and disease outbreaks."[59] Mercury builds on a past program called Open Source Indicators (OSI), which sought to develop "methods for continuous, automated analysis of publicly available data in order to anticipate and/or detect significant societal events, such as political crises, humanitarian crises, mass violence, riots, mass migrations, disease outbreaks, economic instability, resource shortages, and responses to

---

[55] HARRIS, *supra* note 49, at 247; SOLOVE, *supra* note 53, at 184-85. By the time Congress defunded the DARPA version of the program, the administration had changed its name to the less ominous "Terrorism Information Awareness" program. HARRIS, *supra* note 49, at 240, 247.

[56] FRIEDMAN, *supra* note 49; HARRIS, *supra* note 49, at 244, 247, 251-53.

[57] *About IARPA*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, https://www.iarpa.gov/index.php/about-iarpa [https://perma.cc/FS5Y-DW4Z].

[58] *Anticipatory Intelligence*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, *https*://www.iarpa.gov/index.php/about-iarpa/anticipatory-intelligence [https://perma.cc/ZR99-WPU2].

[59] *Mercury*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, https://www.iarpa.gov/index.php/research-programs/mercury [https://perma.cc/BH5P-X8VJ].

natural disasters."[60] Similarly, IARPA's Cyber-attack Automated Unconventional Sensor Environment (CAUSE) program seeks to develop "new automated methods that forecast and detect cyber-attacks significantly earlier than existing methods."[61] CAUSE seeks to use "earlier attack phases, such as target reconnaissance, planning, and delivery," to "enable warning of significant cyber events prior to their most damaging phases."[62]

IARPA's OSI project yielded an automated system that predicts significant societal events based on open-source data. The system, Early Model-Based Event Recognition using Surrogates (EMBERS), generates real-time forecasts of significant societal events such as civil unrest, disease outbreaks, elections, and domestic political crises.[63] EMBERS forecasts include predictions of the day, location, type of event, and participating population.[64] To forecast civil unrest, EMBERS relies on social media data, Wikipedia, news, blogs, and economic data.[65] EMBERS has successfully forecast civil unrest in Brazil, Venezuela, Mexico, Columbia, and Paraguay.[66]

Other researchers working on an IARPA grant took a simpler approach to predicting civil protests across Latin America from 2011 to 2014. They found that, by calculating both the volume and the rate of change in the volume of certain keywords related to protests, they could use Google Trends data to predict street protests one week in advance.[67]

---

[60] *Open Source Indicators*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, https://www.iarpa.gov/index.php/research-programs/osi [https://perma.cc/7J9W-XUXQ].

[61] *Cyber-attack Automated Unconventional Sensor Environment*, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, https://www.iarpa.gov/index.php/research-programs/cause [https://perma.cc/WCL5-7DYF].

[62] *Id.*

[63] NAREN RAMAKRISHNAN ET AL., MODEL-BASED FORECASTING OF SIGNIFICANT SOCIETAL EVENTS 86 (IEEE Intelligent Systems 2015).

[64] *Id.* at 86.

[65] *Id.* at 87.

[66] Sathappan Muthiah et al., *EMBERS at 4 years: Experiences operating an Open Source Indicators Forecasting System*, *in* PROC. OF THE 22ND ACM SIGKDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 205, 208-10 (2016), http://dx.doi.org/10.1145/2939672.2939709 [https://perma.cc/8SAH-ZGW8].

[67] Hong Qi et al., *Open source data reveals connection between online and on-street protest activity*, 5 EPJ DATA SCI. vol. 18, 2016, at 1, 3-4,

IARPA is not the only government agency funding research into predicting terrorism. Horizon 2020, the European Union's research funding initiative, funds a wide array of programs intended to secure Europe's global competitiveness and security.[68] Horizon 2020's most recent call for proposals sought projects that would generate "policy recommendations and tools aimed at improving their ability to prevent and detect radicalization by national and local security practitioners in a timely manner, i.e. before individuals turn towards violent, criminal or terrorists [sic] acts."[69]

Given the extent of the prediction-based research agenda and the critical nature of the terrorist threat, the government would likely find the political will to implement predictive surveillance if it were a promising tool. It is less clear whether the public would tolerate the use of predictive surveillance for ordinary law enforcement, though the public might accept a program focused on predicting mass shootings and other high-casualty crimes. To be sure, government will always have incentives to expand its use of investigative tools, and limiting investigatory techniques to specific crimes may be challenging. However, as predictive analytics takes even deeper root in individuals' lives, some segments of the public may come to believe that terrorism and even some general crime prevention efforts should benefit from the same analytical tools as marketers, insurers, and financial institutions. The balance of this Article, therefore, discusses how existing Fourth Amendment doctrine might accommodate predictive surveillance and assesses the extent to which these accommodations threaten to destabilize Fourth Amendment doctrine itself. This Article identifies the narrowest possible way to authorize predictive surveillance so that it does not become the thin edge of the wedge that pries open Fourth Amendment jurisprudence.

---

https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-016-0081-5 [https://perma.cc/PRQ6-YK5J].

[68] *What is Horizon 2020?*, EUR. COMM'N, http://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020 [http://perma.cc/QBK6-MKAE].

[69] Horizon 2020 Work Programme 2016-17, *14. Secure societies – Protecting freedom and security of Europe and its citizens*, EUR. COMM'N 1, 23 (2017), http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf [https://perma.cc/E3ZL-22A6].

III. PREDICTIVE SURVEILLANCE AND THE THREAT TO EXISTING SURVEILLANCE REGULATION

Predictive surveillance does not fit the existing model of surveillance regulation. Nevertheless, given the high stakes of surveillance programs promising to prevent domestic terrorism and serious crimes, courts will feel pressure to authorize the programs. That pressure may lead courts to distort Fourth Amendment doctrine itself. This Part discusses why predictive surveillance poses such a threat and shows how past courts twisted seemingly-plain statutory language to accommodate mass surveillance.

Two factors contribute to the threat that predictive surveillance poses to existing surveillance law. The first factor is the lack of individualized suspicion at the data collection phase, which puts predictive surveillance at odds with the existing framework of surveillance regulation. Existing surveillance law first evaluates whether the government can demonstrate sufficient suspicion about the surveillance target. For example, the traditional Fourth Amendment search and seizure analysis asks whether the target of the search enjoys a reasonable expectation of privacy.[70] Similarly, before the government can intercept wire or electronic communications, the Electronic Communications Privacy Act requires the government to show probable cause to believe that the target has committed or will commit a specified offense.[71] Under the Foreign Intelligence Surveillance Act, the government must demonstrate that the surveillance target is "a foreign power or an agent of a foreign power."[72] And even under FISA's more permissive business records provision, the government must still demonstrate reasonable grounds that the records it seeks are "relevant to an authorized investigation" to obtain foreign intelligence information or to protect against international terrorism.[73]

Predictive surveillance, however, rests on the opposite premise. At the point of collection the government has no suspicion about any particular subject. Instead, the goal is to collect all of the data, identify

---

[70] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[71] 18 U.S.C. § 2518(3)(a) (2012).

[72] 50 U.S.C. § 1805(a)(2)(A) (2012).

[73] 50 U.S.C. § 1861(b)(2)(A) (2012).

predictive patterns, and use those patterns later to prevent future terrorist or criminal activity.[74] The current approach to surveillance regulation cannot accommodate a predictive surveillance model in which the first step is to analyze *all* the data for patterns that could later yield individualized suspicion.

The second factor contributing to the threat that predictive surveillance poses to existing surveillance law is the emotional appeal of pro-surveillance arguments. Unsurprisingly, surveillance proponents frame their arguments in stark terms emphasizing the dire consequences of a terrorist attack.[75] These arguments have deep emotional appeal. Recall the effect of National Security Advisor Condoleezza Rice's warning before the second Iraq war about the risk that Saddam Hussein possessed weapons of mass destruction: "We do not want the smoking gun to be a mushroom cloud."[76] As former NSA General Counsel Stuart Baker recognized just months after 9/11, "If using more intrusive technology is the only way to prevent horrible crimes, chances are that we'll decide to use that technology, and then adjust our sense of what is private and what is not."[77] Charlie Savage's coverage of post-9/11 surveillance regulation proved Baker correct. Savage observed that "[t]he history of the FISA Court revealed after the Snowden leaks showed that it often seemed to rubber-stamp what the NSA wanted to do."[78]

These two risk factors likely led the Foreign Intelligence Surveillance Court to twist the language of the USA PATRIOT Act beyond recognition in order to approve the NSA's bulk telephone

---

[74] *See* Shaun B. Spencer, *When Targeting Becomes Secondary: A Framework for Regulating Predictive Surveillance in Anti-Terrorism Investigations*, 92 DENV. U. L. REV. 493, 504 (2015).

[75] *See* Shaun B. Spencer, *Security Versus Privacy: Reframing the Debate*, 79 DENV. U. L. REV. 519, 519 (2002).

[76] Wolf Blitzer, *Search for the 'Smoking Gun'*, CNN.COM (Jan. 10, 2003), http://www.cnn.com/2003/US/01/10/wbr.smoking.gun/ [http://perma.cc/G8FU-8988].

[77] David Streitfeld & Charles Piller, *Big Brother Finds Ally in Once-Wary High Tech*, L.A. TIMES (Jan. 19, 2002), http://articles.latimes.com/2002/jan/19/news/mn-23644 [https://perma.cc/K6PF-58GT].

[78] CHARLIE SAVAGE, POWER WARS 573 (2015). For example, after excoriating the government for systemically violating FISC-imposed rules for handling the bulk email program (Section 702), the FISC nevertheless granted the NSA's request to restart the program (which had lapsed after systematic violations) and to "collect and use the wider swath of information going forward." *Id.* at 564-65.

metadata collection program. Under Section 215 of the USA PATRIOT Act,[79] the government may not obtain an order to produce business records without showing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[80] In 2006, in an effort to find statutory authority for the bulk telephone metadata collection program that the Bush administration began after 9/11, the government sought a Foreign Intelligence Surveillance Court order directing telecommunication companies to provide bulk call detail records pursuant to Section 215.[81] The government argued that all of the call detail records were relevant because the NSA could not conduct metadata analysis unless it first collected all of the data.[82] The FISC granted the government's application in an order that contained no legal analysis.[83] The FISC repeatedly reauthorized the government's applications over the next eight years, although no FISC judge offered any legal analysis until after Edward Snowden revealed the existence of the program and the FISC's authorization.[84]

The FISC's secret interpretation strained the term "relevant" beyond recognition. First, interpreting relevance to include data on

---

[79] USA PATRIOT Act § 215, 50 U.S.C. § 1861 (2012).

[80] 50 U.S.C. § 1861(b)(2)(A).

[81] PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 21-22, (2014) (hereinafter "PCLOB REPORT"), available at http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program.pdf [https://perma.cc/XT4G-F9D3] [hereinafter PCLOB REPORT].

[82] PCLOB REPORT, *supra* note 81, at 43.

[83] *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 06-05 (FISA Ct. May 24, 2006), https://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf [http://perma.cc/5W5N-K6ZQ].

[84] *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-109 (FISA Ct. Aug. 29, 2013) (amended memorandum opinion), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf [https://perma.cc/VFD7-YQ8G].

every telephone call rendered the term meaningless.[85] Second, the text of Section 215 itself included three illustrations of records that were "presumptively relevant to an authorized investigation": records pertaining to (1) a foreign power or agent thereof, (2) activities of a suspected agent of a foreign power who is the subject of the authorized investigation, and (3) an individual in contact with or known to such a suspected agent of a foreign power.[86] None of these examples are consistent with so broad an interpretation of the term "relevant." Finally, the drafter of the USA PATRIOT Act, former Republican House member James Sensenbrenner, confirmed that Congress intended to *prevent* the government from using Section 215 to engage in bulk collection.[87]

Predictive surveillance will present an even stronger motivation for shoehorning bulk collection into the traditional surveillance regulation model. The NSA bulk telephone metadata collection program offered the government a fallback position. Rather than collecting all of the data from the telecommunications providers in advance, the government could instead have made individual requests from each provider about each subject of interest. In fact, that is precisely the approach that Congress took in the post-Snowden reform legislation. The USA FREEDOM Act prohibited bulk collection under Section 215, and instead required the government to conduct its "contact chaining" analysis by obtaining records on a case-by-case basis directly from the telecommunications companies.[88] For predictive analytics, however, there is no such fallback position. Either the government collects all of the data, or it cannot conduct the analysis.

Hard cases often make bad law, and evaluating predictive surveillance under the existing surveillance regulation framework will likely present a very hard case. The rest of this Article discusses the avenues that courts could take to authorize the bulk collection required

---

[85] *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL'Y 757, 841 (2014) ("It would be impossible to establish that all customer and subscriber records pertain to a foreign power or an agent thereof, or to a particular, suspected agent of the same, who is the subject of an authorized investigation. Perhaps five or ten customers may fall into this category, but to include millions simply pushes the bounds of common sense. Accordingly, the telephony metadata are neither relevant nor presumptively relevant.").

[86] USA PATRIOT Act § 215, 50 U.S.C. § 1861(b)(2)(A) (2012).

[87] Brief Amicus Curiae of Congressman F. James Sensenbrenner, Jr. in Support of Plaintiffs at 2–4, ACLU v. Clapper, 959 F. Supp. 2d 724 (No. 13 Civ. 3994 (WHP)).

[88] USA FREEDOM Act § 103, 50 U.S.C. § 1861 (2012).

for predictive surveillance and analyzes which of those avenues would least disrupt Fourth Amendment jurisprudence.

IV. PREDICTIVE SURVEILLANCE AND THE THIRD-PARTY AND PUBLIC-EXPOSURE DOCTRINES

Part IV first summarizes the third-party and public-exposure doctrines and identifies potential exceptions that courts have begun to explore. Next, this Part considers the implications of the various approaches that courts could take to apply these doctrines to the data collection necessary for predictive surveillance.

A. *The Third-Party and Public-Exposure Doctrines*

The Fourth Amendment's protection against unreasonable searches applies only where the court determines that an individual enjoys a reasonable expectation of privacy.[89] Under the third-party doctrine, people enjoy no expectation of privacy in information shared with third parties, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[90] Accordingly, there is no Fourth Amendment protection for information such as telephone numbers that an individual dialed[91] or bank account records held by the bank.[92] Similarly, under the public-exposure doctrine,[93] people enjoy no expectation of privacy in information that

---

[89] *E.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[90] United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 752 (1971)); *see also* Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963).

[91] Smith v. Maryland, 442 U.S. 735, 743 (1979) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[92] *Miller*, 425 U.S. at 443.

[93] Although the Court itself does not use this label, commentators have used it to describe cases holding that individuals lack any reasonable expectation of privacy in what they expose to the public. *See, e.g.*, Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 674 (1988); Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 709 (2015).

they knowingly expose to the public.[94] Thus, there is no Fourth Amendment protection for one's movements along public roads (at least when monitored over a short period of time)[95] or for areas of one's property visible from an airplane or a helicopter.[96]

The Supreme Court has wrestled with how to apply the public-exposure doctrine to long-term location tracking. In *United States v. Jones*, the thirty-day aggregation of location data about a single individual was enough to overcome the general rule that one lacks an expectation of privacy in one's location in public spaces.[97] The aggregation in *Jones* would pale in comparison to the massive aggregation necessary for predictive surveillance. For example, the NSA's Section 215 bulk telephone metadata program collected and stored five years of metadata on American telephone users' calls.[98] Similarly, a national network of automated license plate readers could create a catalog showing where every car in the country traveled for as long as the program operated.[99]

In addition, Justice Sotomayor's concurrence in *Jones* raised questions about whether the third-party doctrine is well suited to the digital age.[100] Although the Supreme Court has not yet tackled this issue, a few lower courts have resisted applying the third-party doctrine in some circumstances. For example, the Sixth Circuit held that the third-party doctrine did not deprive an individual of a reasonable expectation of privacy in emails stored in the hands of an email

---

[94] Katz v. United States, 389 U.S. 347, 351 (1967).

[95] United States v. Jones, 565 U.S. 400, 418-19 (2012) (Alito, J. & Sotomayor, J., concurring); United States v. Knotts, 460 U.S. 276, 281-82 (1983).

[96] California v. Ciraolo, 476 U.S. 207, 213-15 (1986); Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986); Florida v. Riley, 488 U.S. 445, 451 (1989).

[97] *Jones*, 565 U.S. at 413-17 (Sotomayor, J., concurring); *id.* at 418 (Alito, J., concurring).

[98] Scott Shane, *N.S.A. Violated Rules on Use of Phone Logs, Intelligence Court Found in 2009*, N.Y. TIMES, Sept. 11, 2013, at A14.

[99] For a discussion of widespread uses of automatic license plate readers, see generally ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 7–15 (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [https://perma.cc/ZXT4-WJCB].

[100] *Jones*, 565 U.S. at 417-18.

service,[101] and the Ninth Circuit held that the mere fact that others had occasional access a computer connected to a university network did not deprive the computer user of a reasonable expectation of privacy.[102] Given the narrow circumstances of *Jones*, the Supreme Court has wide latitude to decide how to apply the third-party and public-exposure doctrines to any type of mass surveillance.

With its recent grant of certiorari in *United States v. Carpenter*, the Court is poised to decide whether the third-party doctrine applies to gathering long-term cell site location information from a cellular telephone provider.[103] The *Carpenter* decision could significantly impact how future courts approach predictive surveillance. If the Court holds that long-term CSLI collection does not fall within the third-party doctrine, that would make it more difficult for courts to find predictive analytics data collection to fall within the third-party doctrine. On the other hand, even a holding that long-term CSLI collection falls within the third-party doctrine would not necessarily compel the same decision for mass surveillance given the far broader scope of data collection at issue.

B. *A Sweeping Approach to Predictive Surveillance Under the Third-Party and Public-Exposure Doctrines*

The simplest way to approve predictive surveillance would be a literal application of the third-party and public-exposure doctrines. Under such an approach, the court would reason that any information shared with third parties or exposed to the public is unprotected under the Fourth Amendment, no matter how long-term or pervasive the surveillance.

The only opinions to date applying the third-party doctrine to mass surveillance involve challenges to the NSA's bulk telephone metadata collection program. Both the Southern District of New York and the Foreign Intelligence Surveillance Court held that the third-party doctrine shielded the bulk metadata collection program from Fourth

---

[101] United States v. Warshak, 631 F.3d 266, 286-87 (6th Cir. 2010).

[102] United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007).

[103] United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

Amendment scrutiny.[104] In *ACLU v. Clapper*, Judge Pauley of the Southern District of New York rejected the idea that bulk collection of telephone metadata distinguished the case from the handful of phone numbers dialed in *Smith v. Maryland*: "The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[105] Judge Pauley also rejected the ACLU's argument that the database gave the government a "rich mosaic" of each person's life.[106] Judge Pauley reasoned that merely collecting the numbers did not paint that mosaic because the government cannot query the database without tying that query to an approved target.[107] The Foreign Intelligence Surveillance Court took a similar approach when it approved orders implementing the Section 215 bulk telephone metadata collection program.[108]

---

[104] ACLU v. Clapper, 959 F. Supp. 2d 724, 749–52 (S.D.N.Y. 2013), *vacated*, 785 F.3d 787, 826 (2d Cir. 2015) (holding that Section 215 did not authorize bulk collection); *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13–109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013).

[105] *Clapper*, 959 F. Supp. 2d at 752. This sentiment, however, ignores the approach of five Justices in *United States v. Jones*. For those justices, short-term tracking of one's public movements did not trigger the Fourth Amendment, but long-term tracking of those same movements did. *Jones*, 565 U.S. at 418-19, 431 (Alito, J., concurring joined by Ginsburg, Breyer & Kagan, JJ.); *id.* at 415 (Sotomayor, J., concurring) (agreeing with Justice Alito that long-term GPS tracking violates the Fourth Amendment's reasonable expectation of privacy).

[106] *Clapper*, 959 F. Supp. 2d at 750–51.

[107] *Id.* at 750–51.

[108] *See, In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13–109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013). The circuit courts never had to reach the Fourth Amendment issue because Section 215 sunset on June 1, 2015, and was replaced by the USA FREEDOM Act, which prohibits bulk collection and takes effect on November 28, 2015. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268; *In re* Application of the FBI, Bankr. No. 15-75, 2015 WL 5637562, at *4–5 (FISA Ct. June 29, 2015). The only circuit courts to consider the bulk telephone metadata program ruled on other grounds. ACLU v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015) (rejecting government's proposed interpretation of term "relevant" in Section 215); Obama v. Klayman, 800 F.3d 559, 568, 570 (D.C. Cir. 2015) (vacating preliminary injunction based on plaintiffs' failure to demonstrate likelihood of success on standing issue).

On the other hand, in *Klayman v. Obama*,[109] Judge Leon reasoned that "the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies" justified distinguishing *Smith v. Maryland*.[110] He relied in part on the fact that the NSA's bulk collection constituted a massive aggregation of data.[111] In this regard, he analogized to *United States v. Jones*,[112] where five concurring Justices emphasized the significance of aggregating an individual's GPS data.[113] Judge Leon applied the same aggregation idea to distinguish *Smith v. Maryland*. The pen register in *Smith* only tracked a single defendant's telephone metadata for a day,[114] but the Section 215 bulk collection program built a comprehensive, five-year record of Americans' phone calls.[115] For Judge Leon, this was a difference not merely in degree, but in kind.[116]

If the Court held that predictive surveillance data collection fell within the third-party and public-exposure doctrines, that would dramatically expand those doctrines. There would be nothing other than political opposition to prevent the government from collecting every scrap of data visible to the public or shared with a third party. The risk of such unbridled surveillance power appeared to give Chief Justice Roberts pause at oral argument in *Jones*, when he asked the government whether accepting its argument meant that the government was free to place GPS trackers on the justices' cars.[117] Given

---

[109] Obama v. Klayman, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated on other grounds*, 800 F.3d 559, 560 (D.C. Cir. 2015) (vacating preliminary injunction based on plaintiffs' failure to demonstrate likelihood of success on standing issue).

[110] *Id.* at 31.

[111] *Id.* at 32.

[112] United States v. Jones, 565 U.S. 400 (2012).

[113] *Klayman*, 957 F. Supp. 2d at 31 (citing *Jones*, 565 U.S. at 415-18 (Sotomayor, J., concurring)); *Jones*, 565 U.S. at 430 (Alito, J., concurring joined by Ginsburg, Breyer & Kagan, JJ.).

[114] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[115] *Klayman*, 957 F. Supp. 2d at 32.

[116] *Id.* at 32–33, 37.

[117] Transcript of Oral Argument at 9:18 to 10:30, United States v. Jones, 131 S. Ct. 3064 (2011) (No. 10-1259) (Roberts, C.J.), http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf

the Court's concerns about data aggregation on a much smaller scale in *Jones* and *Riley*,[118] there is reason to believe that the Court would shy away from this most extreme avenue to approving predictive surveillance.

C. *A More Nuanced Approach to Predictive Surveillance and the Third-Party and Public-Exposure Doctrines*

A more nuanced approach would recognize that, at a minimum, the massive data aggregation required by predictive surveillance should override the third-party and public-exposure doctrines. This Article proposes that the third-party doctrine should not apply to the type of bulk collection necessary for predictive analytics. As I have argued elsewhere, the third-party doctrine is flawed because it represents an "all or nothing" approach to privacy that ignores reality in several significant ways.[119]

First, the third-party doctrine fails to distinguish third parties as ends from third parties as means.[120] In the case that spawned the third-party doctrine, *United States v. Miller*,[121] the Court relied on its earlier "misplaced trust" cases.[122] Under those cases, the Court warned that people who share information with acquaintances take a risk that those acquaintances may abuse their trust and tell others, including the police.[123] But by extending that logic to the telephone numbers dialed in *Smith v. Maryland*,[124] the Court ignored the difference between ends and means. In the misplaced trust cases, the communication to an

---

[https://perma.cc/TU8F-5NJ9].

[118] *See* United States v. Jones, 565 U.S. 400, 415, 430 (2012) (Alito, J., concurring & Sotomayor, J., concurring); Riley v. California, 134 S. Ct. 2473, 2491 (2014). For a discussion of the role of aggregation in *Jones* and *Riley*, see *infra* text at notes 128–37.

[119] Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 401 (2013).

[120] *Id.* at 401–02.

[121] United States v. Miller, 425 U.S. 435 (1976).

[122] *Id.* at 443–44 (citing United States v. White, 401 U.S. 745, 751–52 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963).

[123] *White*, 401 U.S. at 751–52; *Hoffa*, 385 U.S. at 302; *Lopez*, 373 U.S. at 438.

[124] *See* Smith v. Maryland, 442 U.S. 735, 741–46 (1979).

untrustworthy acquaintance is both the end and the means. But the telephone company's record of the numbers that its customers dialed is merely the means to a different end—the communication with an acquaintance.[125]

Second, the third-party doctrine ignores what I have called the "anti-aggregation norm."[126] This visceral, societal fear of pervasive surveillance is a common theme in both literature and legal commentary.[127] And it figured prominently in *Riley v. California*,[128] where the Court rejected law enforcement's attempt to apply the search incident to arrest doctrine to cell phone data.[129] Under that doctrine, when law enforcement officers arrest a suspect, they may search personal property on the arrestee's person or within his immediate control without a warrant.[130] This exception to the probable cause requirement exists (1) to protect the arresting officers from harm and (2) to prevent the destruction of evidence.[131] The Court refused to apply the exception to cell phones for two reasons. First, the Court reasoned that searching a cell phone would not serve the doctrine's purposes because a cell phone neither threatens officer safety nor triggers a need to preserve evidence.[132] Second, the Court reasoned that the vast aggregation of data found within a cell phone rendered a cell phone search far more intrusive than a physical search of objects on one's person.[133]

---

[125] *See* Commonwealth v. Augustine, 4 N.E.3d 846, 861–63 (Mass. 2014) (citing State v. Earls, 214 N.J. 564, 587 (2013)) (refusing to apply the third-party doctrine to cell site location information because individuals do not intend to voluntarily transmit their location to the cell service provider when making a call and location information bears no relation to the communicative purpose of the call).

[126] Spencer, *Surveillance Society*, *supra* note 119, at 402–03 (discussing privacy themes in George Orwell's *Nineteen Eighty-Four* and Franz Kafka's *The Trial*).

[127] *Id.*

[128] Riley v. California, 134 S. Ct. 2473 (2014).

[129] *Id.* at 2485.

[130] *Id.* at 2482–84.

[131] *Id.* at 2483–84.

[132] *Id.* at 2485–87.

[133] *Id.* at 2489.

The anti-aggregation norm also lies at the heart of the concurring opinions that rejected long-term, warrantless GPS tracking in *United States v. Jones*. Justice Alito recognized that short-term location monitoring would not violate one's reasonable expectation of privacy. However, when the tracking lasted for four weeks, this long-term tracking exceeded one's reasonable expectation of privacy because "society's expectation has been that law enforcement agents and others would not – and indeed, in the main, simply could not – secretly monitor and catalogue every single movement of an individual's car for a very long period."[134] And Justice Sotomayor reasoned that people should not have to "expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[135] Although *Riley* and *Jones* answered different legal questions,[136] they both relied on the notion that the aggregation of data can give rise to Fourth Amendment protection, even if the individual data points would not merit such protection. For that reason, commentators have characterized both *Riley* and the *Jones* concurrences as evoking the mosaic theory, which is "premised on aggregation [in that] it considers whether a set of non-searches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic."[137]

---

[134] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring) (agreeing with Justice Alito that long-term monitoring violates one's expectation of privacy).

[135] *Id.* at 415-16 (Sotomayor, J., concurring); Commonwealth v. Augustine, 4 N.E.3d 846, 862–63 (Mass. 2014) (declining to apply the third-party doctrine to cell site location data obtained from a cell phone provider and reasoning that "even CSLI limited to the cell site locations of telephone calls made and received may yield a treasure trove of very detailed and extensive information about the individual's 'comings and goings' in both public and private places").

[136] Indeed, in *Riley*, the Court declined to address "whether the collection or inspection of aggregated digital information amounts to a search under other circumstances [than a search incident to arrest]." *Riley*, 134 S. Ct. at 2489-90 n.1.

[137] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012). For the proposition that both *Riley* and the *Jones* concurrences invoke the mosaic theory, *see* Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 206-08 (noting that both *Riley* and the *Jones* concurrences "talk about privacy in mosaic-theory terms"); Ric Simmons, *The Missed Opportunities of Riley v. California*, 12 OHIO ST. J. CRIM. L. 253, 2622-64 (2014) ("[i]n both *Jones* and *Riley*, the Court is getting close to adopting the 'mosaic theory'"); Robert Greenleaf Brice & Katrina L. Sifferd, *Domestic Drone Surveillance: The Court's Epistemic Challenge and Wittgenstein's Actional*

Finally, the third-party doctrine rests on a flawed assumption that the third-party disclosure assumes the risk of further disclosure.[138] In *United States v. Miller*, the Court relied on the notion that bank and telephone customers voluntarily assume the risk that third parties will disclose their information.[139] Even if this reasoning justified an all-encompassing third-party doctrine four decades ago, it does not hold true today. First, consumers do not have a meaningful choice about whether to use services that involve sharing data with third parties.[140] And second, even if consumers did have a choice, they would lack the information needed to exercise that choice.[141]

Given the risks posed by mass surveillance, courts should not put predictive surveillance beyond constitutional reach by holding that it falls within the third-party and public-exposure doctrines. Such a sweeping approach would entrench the third-party and public-exposure doctrines in every conceivable context. Even for courts predisposed to approve predictive surveillance, the sounder approach would be to refuse to apply the third-party and public-exposure doctrines and instead adopt one of the reasonableness approaches discussed below. This would give courts more control over when

---

Certainty, 77 LA. L. REV. 805, 827 (2017) (noting that Justice Sotomayor's concurrence in *Jones* and the *Riley* opinion reflect the mosaic theory). *Riley*, of course, did not rely solely on the mosaic theory. *Riley* also noted that cell phones are likely to hold uniquely personal types of data such as internet search and browsing history, historic location information, and other detailed information about one's life, and that cell phones also provide access to vast amounts of data stored in the cloud rather than on the device itself. *Riley*, 134 S. Ct. at 2490-91. In addition, although Justice Sotomayor's concurrence in *Jones* explicitly invoked the mosaic theory, Justice Alito's concurrence may be read more narrowly. *Jones*, 565 U.S. at 430 (Alito, J., concurring). He did not rely explicitly on the portrait of one's life that four weeks of location tracking could yield. *Id.* Instead, he drew a purely expectation-based distinction by reasoning that people expect law enforcement to engage in short-term but not long-term location tracking. *Id.*

[138] Spencer, *supra* note 119, at 404–05.

[139] United States v. Miller, 425 U.S. 435, 442–43 (1976).

[140] Spencer, *supra* note 119, at 404–05. Justice Marshall advanced precisely this argument in *Smith v. Maryland*, albeit unsuccessfully. Smith v. Maryland, 442 U.S. 73535, 749-50 (1979) (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice. . . . [H]ere, unless a person is prepared to forego use of what for many has become a personal or professional necessity [i.e., the telephone], he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.") (citations omitted).

[141] Spencer, *supra* note 119, at 405–06.

predictive surveillance was or was not justified, while also allowing the third-party and public-exposure doctrines to adapt to the digital era. Accordingly, the next Part considers how courts could apply the Fourth Amendment's reasonableness requirement to predictive surveillance.

V. PREDICTIVE SURVEILLANCE AND THE REASONABLENESS REQUIREMENT

This Part discusses how future judicial approval of predictive surveillance could affect the Fourth Amendment reasonableness requirement. It first summarizes the reasonableness requirement and the general rule that reasonableness demands a warrant issued upon probable cause. Next, it discusses several different exceptions to the warrant requirement and considers the implications of relying on each exception to authorize predictive surveillance.

A. *The Reasonableness Requirement*

In the law enforcement context, reasonableness under the Fourth Amendment generally requires that officers obtain a warrant supported by probable cause that the search will reveal evidence of a particular crime.[142] The Supreme Court, however, has developed numerous exceptions to the warrant requirement.[143] Although these exceptions vary in their particulars, they each purport to apply the Fourth Amendment's requirement that searches and seizures be reasonable.[144] To assess reasonableness, courts balance the government's interest in the search against the nature of the intrusion on individual liberties.[145]

The reasonableness analysis highlights the difference between traditional and predictive surveillance. Even where the Court does not

---

[142] *E.g.*, United States v. Leon, 468 U.S. 897, 913–15 (1984).

[143] Examples of these exceptions include searches incident to lawful arrest, plain view searches, searches in exigent circumstances, inventory searches, and administrative searches. David C. Behar, *An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context*, 66 U. MIAMI L. REV. 471, 472 (2012).

[144] STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE 32 (9th ed. 2010) ("When an exception to the warrant requirement is applicable, only the reasonableness requirement must be satisfied.").

[145] *E.g.*, Illinois v. Lidster, 540 U.S. 419, 426-27 (2004); Terry v. Ohio, 392 U.S. 1, 21, 24 (1968).

require a warrant issued upon probable cause, the reasonableness requirement usually demands some degree of individualized suspicion.[146] Predictive surveillance by its nature is incompatible with the warrant and probable cause standard because, by definition, the government has no particularized suspicion about the subjects of the surveillance. In theory, courts could simply reason that there is neither probable cause nor even reasonable suspicion for bulk data collection, and therefore predictive surveillance can never meet the Fourth Amendment's reasonableness requirement. Such a dogmatic approach seems highly unlikely as well as unduly restrictive if the technology has the potential to deter terrorism or crime. Therefore, courts predisposed to authorize some form of predictive surveillance are likely to rely on or expand existing exceptions to the warrant requirement.

B. *A Terry-Style Exception to the Warrant and Probable Cause Requirement for Predictive Surveillance*

The most sweeping doctrinal approach to finding predictive surveillance reasonable would carve out an exception similar to the stop and frisk exception in *Terry v. Ohio*.[147] Although the stop and frisk shares almost nothing in common with predictive surveillance, the techniques do share one feature from the perspective of Fourth Amendment law: neither fits neatly into the traditional categories of Fourth Amendment doctrine. Just as the Supreme Court created an exception to bridge that doctrinal disconnect in *Terry*, courts could create a similar exception for predictive surveillance.

In *Terry*, the Court considered how to apply the Fourth Amendment to the stop and frisk, a technique in which an officer stops a suspect for questioning and frisks the person if he has reason to believe the suspect is armed.[148] The technique did not fit neatly into the existing Fourth Amendment doctrine when the Court first confronted

---

[146] *See Terry*, 392 U.S. at 30-31 (requiring reasonable belief that criminal activity is afoot and suspect is armed before conducting stop and frisk); New Jersey v. T.L.O., 469 U.S. 325, 340-41 (1985) (requiring reasonable grounds to suggest student violation of law or school rules before searching student); Camara v. Municipal Court, 387 U.S. 523, 537-38 (1967) (requiring some reason such as passage of time, type of building, or condition of neighborhood before conducting housing code inspection).

[147] Terry v. Ohio, 392 U.S. 1 (1968).

[148] *Id.* at 10.

it.[149] The defendant argued that the police could not stop and frisk him without a warrant based on probable cause.[150] Yet the Court recognized that the stop and frisk took place in circumstances where obtaining a warrant was impractical.[151] The government argued that the stop and frisk did not constitute a search or seizure under the Fourth Amendment.[152] Yet, such a categorical approach would have placed significant police infringements on individual freedom beyond constitutional regulation.[153]

The Court rejected a "rigid all-or-nothing model" of the Fourth Amendment[154] and instead adopted a compromise grounded in the reasonableness determination.[155] That reasonableness determination required the Court to balance the government's interest against the nature of the intrusion on individual rights.[156] *Terry* and its progeny treated the initial detention as a Fourth Amendment seizure and the weapons frisk as a Fourth Amendment search,[157] but the Court created a lower standard of individualized suspicion to satisfy the Fourth Amendment's reasonableness requirement.[158] The initial detention does not require probable cause; instead, the officer need only have reasonable suspicion that criminal activity "may be afoot."[159] In light of the law enforcement interest in investigating crime, the brief

---

[149] *Id.* at 9-10; WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 9.1(a) (5th ed. 2016) ("what the police viewed as a distinct procedure did not fit comfortably within any extant legal pigeonhole").

[150] *Terry*, 392 U.S. at 11.

[151] *Id.* at 20.

[152] *Id.* at 10.

[153] *See, id.* at 17 & n.15.

[154] *Id.* at 17.

[155] *Id.* at 18-19.

[156] *Id.* at 21, 24, 27.

[157] *Id.* at 19; Adams v. Williams, 407 U.S. 143, 145-46 (1972).

[158] *Terry*, 392 U.S. at 30.

[159] *Id.*

investigatory stop is reasonable.[160] Similarly, the weapons frisk does not require probable cause; instead, the officer must have reasonable grounds to believe the suspect is armed.[161] Although the weapons frisk is a significant intrusion, that intrusion is reasonable in light of the government's interest in officer safety.[162]

Courts confronting predictive surveillance for the first time may take a similar approach to the stop and frisk in *Terry*. Had the *Terry* Court required probable cause, it would have rendered nearly all stop and frisks unconstitutional. Similarly, requiring the government to demonstrate particularized suspicion before undertaking predictive surveillance would effectively ban predictive surveillance because predictive surveillance, by definition, lacks particularized suspicion.

Following *Terry*'s model, courts could balance the governmental interest in predictive surveillance against the nature of the intrusion. As to the governmental interest, courts could require the government to demonstrate a reasonable likelihood that predictive surveillance would reveal terrorist or criminal activity.[163] Such a requirement would be analogous to *Terry*'s requirement of reasonable suspicion that criminal activity is afoot. Absent such a requirement, the government's asserted interest would be speculative and should not justify an intrusion on individual liberty.

Courts could characterize the nature of the intrusion several different ways. For a broad exception sanctioning predictive surveillance for both counter-terrorism and law enforcement, courts could rely on the fact that the government was collecting information shared with third parties or exposed to the public. Thus, courts would treat the privacy interest as diminished under the circumstances. Such an approach would still credit the notion of assumption of risk underlying the third-party and public-exposure doctrines, but it would not take the drastic position that such information enjoys no Fourth Amendment protection no matter how pervasive the government's data collection practices.

On the other hand, courts could create a narrow exception by emphasizing the massive aggregation of data that predictive surveillance would entail. Just as the aggregation of data heightened

---

[160] *Adams*, 407 U.S. at 146.

[161] *Terry*, 392 U.S. at 30.

[162] *Id.* at 26; *Adams*, 407 U.S. at 146.

[163] *See* Spencer, *supra* note 10, at 528.

the degree of intrusion in *Jones* and *Riley*, the aggregation of data about the entire population – even data shared with third parties or exposed to the general public – would constitute a serious intrusion on individual liberty. In the face of so substantial an intrusion, courts might find predictive surveillance to be reasonable only if the data use were limited to anti-terrorism investigations, or possibly to criminal activity that threatened mass casualties. There is at least some recent support for such an approach. In *United States v. Jones*, where five justices reasoned that long-term, warrantless GPS tracking violated the Fourth Amendment, Justice Alito's concurrence observed that long-term GPS tracking might nevertheless be permissible to investigate "extraordinary offenses."[164] This, however, would be a significant departure from the Supreme Court's refusal to consider the severity of the offense in determining reasonableness under the Fourth Amendment.[165]

---

[164] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring). *Accord* LAFAVE, *supra* note 150, § 9.2(c) ("The *Terry* rule should be expressly limited to investigation of serious offenses.").

[165] For scholarship calling on courts to consider the severity of the offense under investigation in making Fourth Amendment determinations, see David Keenan & Tina M. Thomas, Note, *An Offense-Severity Model for Stop-and-Frisks*, 123 YALE L.J. 1448, 1469 (2014); Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 4 (2011); Eugene Volokh, *Crime Severity and Constitutional Line-Drawing*, 90 VA. L. REV. 1957, 1973-74 (2004); Erik Luna, *Drug Exceptionalism*, 47 VILL. L. REV. 753, 778-87 (2002); William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 847 (2001); Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness"*, 98 COLUM. L. REV. 1642, 1644 (1998); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 784 (1994); William A. Schroeder, *Factoring the Seriousness of the Offense into Fourth Amendment Equations – Warrantless Entries into Premises: The Legacy of* Welsh v. Wisconsin, 38 U. KAN. L. REV. 439, 518 (1990). For cases refusing the call, see for example, United States v. Jones, 565 U.S. 400, 412 (2012) (noting in dicta that "[t]here is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated"); Whren v. United States, 517 U.S. 806, 813 (1996) (upholding detention based on probable cause of traffic violation and "foreclose[ing] any argument that the constitutional reasonableness of traffic stops depends on the actual motivations of the individual officers involved"); Michigan v. Tyler, 436 U.S. 499, 511 (1978) (finding that seriousness of crime does not create exigency justifying warrantless search); Mincey v. Arizona, 437 U.S. 385, 395 (1978) (rejecting "murder-scene" exception to Fourth Amendment warrant requirement despite severity of crime). For an argument that the concurrences in United States v. Jones raise the possibility of crime-severity as a factor in Fourth Amendment reasonableness determinations, see, Scott J. Glick, *Consequence, Weapons of Mass Destruction, and the Fourth Amendment's "No-Win" Scenario*, 90 IND. L.J. 1, 19-20 (2015). *See also* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (dicta) (the

C. *A Lidster-Style Exception to the Warrant Requirement for Predictive Surveillance*

A somewhat narrower doctrinal approach to finding predictive surveillance reasonable would create an exception analogous to the exception for suspicionless, "information-seeking" checkpoints in *Illinois v. Lidster*.[166] Although the scale of predictive surveillance would dwarf the single checkpoint in *Lidster*, they share a common trait: both were conducted without individualized suspicion.

In *Lidster*, the police were investigating a fatal hit-and-run accident on a highway.[167] They set up a checkpoint on the same highway a week later at the same time of night near the location of the accident to try to gather information from the public.[168] The Court recognized that suspicionless checkpoints set up to "detect evidence of ordinary criminal wrongdoing" violated the Fourth Amendment absent special circumstances.[169] However, the Court held that the "information-seeking" checkpoint was not subject to the rule of *City of Indianapolis v. Edmond* prohibiting checkpoints that merely serve a "general interest in crime control."[170] First, the *Lidster* checkpoint merely asked for information about a crime "in all likelihood committed by others," rather than trying to determine whether the vehicle occupants were committing a crime.[171] Next, the *Lidster* Court noted that highway travelers have a somewhat diminished expectation of privacy and that suspicionless highway stops have been allowed for sobriety checks and border patrol stops.[172] Third, the Court reasoned that individualized

---

"Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack").

[166] Illinois v. Lidster, 540 U.S. 419 (2004).

[167] *Id.* at 422.

[168] *Id.* at 422, 427.

[169] *Id.* at 423 (citing City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000)) (holding that checkpoint stopping vehicles to look for evidence of drug crimes violated the Fourth Amendment).

[170] *Lidster*, 540 U.S. at 424 (citing *Edmund*, 531 U.S. at 44).

[171] *Lidster*, 540 U.S. at 423.

[172] *Id.* at 424.

suspicion has no role to play in a purely information-seeking checkpoint, just as it has no role to play in other legitimate police activities like crowd control and public safety.[173] Finally, the Court reasoned that information-seeking checkpoints were inherently less intrusive because they were brief and unlikely to elicit self-incriminating information.[174]

Having distinguished *Edmond*, the Court applied the reasonableness standard by balancing the gravity of the government interest, the degree to which the checkpoint served that interest, and the severity of the intrusion on individual liberty.[175] The Court reasoned that the government interest was grave because they were investigating a fatal crime and because they were investigating a specific, known crime rather than "unknown crimes of a general sort."[176] In addition, the Court noted that the information-seeking checkpoint significantly advanced the governmental interest because the checkpoint took place on the same highway about a week later and at roughly the same time of night as the hit and run.[177] Finally, the Court reasoned that the intrusion on liberty was relatively minimal because it involved just a few minutes of waiting, and because the law enforcement contact involved brief questioning and the distribution of a flyer.[178] On balance, the Court found the information-seeking checkpoint to be reasonable under the Fourth Amendment.

Courts deciding whether predictive surveillance is reasonable under the Fourth Amendment may draw several parallels to *Lidster*. First, predictive surveillance used for counter-terrorism could certainly be seen as going beyond the ordinary needs of law enforcement. Indeed, *Edmond* recognized in dicta that a checkpoint aimed at thwarting a known terrorist attack or catching a dangerous criminal would be permissible.[179] Although the Supreme Court has not opined on whether antiterrorism searches go beyond ordinary law enforcement for

---

[173] *Id.* at 424-25.

[174] *Id.* at 425.

[175] *Id.* at 426-27.

[176] *Id.* at 427.

[177] *Id.* at 427.

[178] *Id.* at 427-28.

[179] City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

purposes of the special needs exception,[180] lower courts have held that they do.[181] To the extent that predictive surveillance also targeted future criminal activity, courts might reason that predicting and deterring future crimes also go beyond ordinary law enforcement. There is at least tangential support for this notion in the Court's cases determining that the probable cause standard did not apply to government intrusions seeking to prevent hazardous conditions.[182] Next, the governmental interest would be far weightier than the interest in *Lidster* if the predictive surveillance scheme were limited to predicting

---

[180] Courts and commentators disagree about whether *Lidster* was a "special needs" case. *Compare* United States v. Amerson, 483 F.3d 73, 80 (2d Cir. 2007) (noting that *Lidster* applied the "special needs doctrine"), *and* David H. Kaye, *Why So Contrived? Fourth Amendment Balancing, Per Se Rules, and DNA Databases After* Maryland v. King, 104 J. CRIM. L. & CRIMINOLOGY 535, 552-53 n.117 (2014) ("*Lidster* is regarded conventionally as a special needs case"), *and* Josh Gupta-Kagan, *Beyond Law Enforcement:* Camreta v. Greene, *Child Protection Investigations, and the Need to Reform the Fourth Amendment Special Needs Doctrine*, 87 TUL. L. REV. 353, 373 (2012) (referring to Lidster as "an earlier special needs case"), *with* Julie Rikelman, *Justifying Forcible DNA Testing Schemes Under the Special Needs Exception to the Fourth Amendment: A Dangerous Precedent*, 59 BAYLOR L. REV. 41, 60 n.131 ("The Second Circuit's treatment of *Lidster* as a special needs case is incorrect. *Lidster* is a checkpoint case, which the Court has explicitly distinguished from those dealing with 'special needs.'"). For present purposes, the label does not matter because both *Lidster* and the special needs doctrine expressly consider whether the suspicionless search serves needs beyond ordinary law enforcement. Illinois v. Lidster, 540 U.S. 419, 423-25 (2004); Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 655 (1995).

[181] *See, e.g.*, United States v. Aukai, 497 F.3d 955, 958-61 (9th Cir. 2007) (upholding pre-boarding search of airline passengers' carry-on baggage); Cassidy v. Chertoff, 471 F.3d 67, 87 (2d Cir. 2006) (upholding random, warrantless searches of ferry commuters' carry-on baggage and vehicles to prevent terrorist attacks); MacWade v. Kelly, 460 F.3d 260, 275 (2d Cir. 2006) (upholding random, suspicionless search of subway passengers' baggage); United States v. Hartwell, 436 F.3d 174, 181 (3d Cir. 2006) (upholding pre-boarding search of airline passengers' carry-on baggage); United States v. Edwards, 498 F.2d 496, 500-01 (2d Cir. 1974) (upholding suspicionless searches of airline passengers' persons and carry-on luggage). For a comprehensive analysis of antiterrorism searches and the special needs exception, see, Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 915-21 (2010) (arguing that suspicionless antiterrorism searches do not fit into the Supreme Court's administrative search or special needs search categories, and proposing that the Court treat an antiterrorism search as lawful under the special needs exception so long as any evidence gathered in the search is excluded from any criminal prosecution).

[182] *See* National Treasury Employees Union v. Von Rabb, 489 U.S. 656, 667 (1989) (customs service trying to prevent drug use by employees in sensitive positions); Board of Education v. Earls, 536 U.S. 822, 834-35 (2002) (school district trying to prevent drug use by students).

terrorism or mass-casualty crimes.[183] And if the government could demonstrate that the predictive surveillance is reasonably likely to identify suspects, then the surveillance would advance the government interest more directly than the suspicionless questioning in *Lidster*. Although predictive surveillance's intrusion upon individual liberties would dwarf the brief questioning in *Lidster*, courts might justify the intrusion based on the magnitude of the governmental interest.

There are, however, conceptual differences between predictive surveillance and the information-seeking checkpoint in *Lidster*. First, *Lidster* did not involve an entirely suspicionless search, because the police were investigating a specific crime in the area one week earlier. Predictive surveillance would seek to predict unspecified future acts. Second, *Lidster* relied in part on the fact that the information-gathering checkpoint did not attempt to elicit evidence that the vehicle occupants had committed the crime. In contrast, predictive surveillance would not only build predictive models; it would also apply those models to emerging data and identify suspects. In light of these differences, courts may have a difficult time fitting predictive surveillance into an exception modeled on *Lidster*.

D. *The Keith Case's Domestic Security Exception to the Warrant and Probable Cause Requirement*

The narrowest way to approve predictive surveillance would be to rely on the rarely litigated exception to the warrant requirement for domestic security investigations. In *United States v. United States District Court* (the *Keith* case), the Supreme Court discussed how the Fourth Amendment applied to the investigation of a CIA office bombing in Michigan.[184] The government tapped the defendant's phones based solely on the Attorney General's approval, rather than obtaining judicial approval.[185] The Supreme Court rejected the government's

---

[183] For a proposal that antiterrorism surveillance should be permissible under the special needs doctrine and that evidence derived from such surveillance should be admissible only in prosecution of terrorism crimes, see, Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289, 1311 (2011). For a proposal that antiterrorism searches should be permissible under the special needs doctrine but that evidence derived from such surveillance should be excluded from any subsequent prosecution, *see* Simmons, *supra* note 182, at 915-21.

[184] United States v. U.S. District Court (Keith), 407 U.S. 297, 299 (1972).

[185] *Id.* at 300-01.

argument that the Fourth Amendment did not apply to domestic security investigations.[186] However, the Court also reasoned that the Fourth Amendment may apply more flexibly in domestic security investigations than in law enforcement investigations.[187] The procedures need only be "reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[188] Ultimately, the Court held that, in light of the intrusion that wiretaps present, wiretaps in domestic security cases require some form of prior judicial approval but need not comply with the strictures of the Wiretap Act.[189]

No court to date has considered whether the *Keith* case's approach to domestic security investigations could apply to bulk data collection. The courts that approved bulk telephone metadata collection simply held that the Fourth Amendment did not apply because of the third-party doctrine.[190] On the other hand, Judge Leon's finding that the program was likely unconstitutional did not consider the Keith case at all.[191] Instead, Judge Leon reasoned that, even if warrantless searches were authorized because of special needs beyond ordinary law enforcement, bulk collection was unnecessary because the government

---

[186] *Id.* at 319-20. Lower courts have relied on *Keith* to define a foreign intelligence exception to the warrant requirement. *See, e.g.*, *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008) ("Applying principles derived from the special needs cases, we conclude that this type of foreign intelligence surveillance possesses characteristics that qualify it for such an exception."); United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980) ("[T]he needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."). Yet predictive surveillance would largely involve domestic data about Americans, and therefore would not fall within a foreign intelligence exception.

[187] *Keith*, 407 U.S. at 323-24.

[188] *Id.* at 323.

[189] *Id.* at 323-24.

[190] *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *2-3 (FISA Ct. Aug. 29, 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 749-52 (S.D.N.Y. 2013).

[191] Klayman v. Obama, 957 F. Supp. 2d 1, 30-42 (D.D.C. 2013).

could seek targeted orders from each of the telecommunications providers.[192]

As a result, the field is wide open for courts to authorize predictive surveillance under the *Keith* case's flexible approach. The *Keith* case teaches that, to collect intelligence for domestic security investigations, the procedures need only be reasonable in relation to the government's need for domestic security intelligence information.[193] The *Keith* case justified a more flexible definition of reasonableness in domestic security investigations because such investigations can involve difficulty in identifying targets and often attempt to prevent future acts.[194] Similar concerns would be present in a predictive surveillance program aimed at counter-terrorism. Developing specific targets would be impossible without first gathering and analyzing all of the data. And the program's purpose would be to prevent future threats to domestic security.

To draft a predictive surveillance regime likely to comply with the *Keith* case, Congress would first have to limit the permissible uses of the information to counter-terrorism and other domestic security threats. If the surveillance could be used for broader purposes, the *Keith* case would not apply at all. Second, Congress would likely have to impose some form of advance judicial approval of the bulk collection. Despite the flexibility of its balancing approach, the Court emphasized the importance of prior judicial approval as a check upon executive branch discretion.[195] Given the Court's recognition that the form of prior judicial approval may adapt to the government interest in domestic security cases,[196] Congress could require a prior judicial finding that predictive surveillance was likely to reveal patterns associated with counter-terrorism or domestic security threats.

Relying on the *Keith* case to authorize predictive surveillance would have the laudable effect of limiting the permissible uses of such a powerful technology. This might mean sacrificing the ability to prevent some types of criminal activity that predictive surveillance could detect.

---

[192] *Id.* at 38–41.

[193] *Keith*, 407 U.S. at 322-24.

[194] *Id.* at 322.

[195] *Id.* at 316-18.

[196] *Id.* at 321-23.

Such a limitation offers a reasonable tradeoff in light of the sweeping data collection that predictive surveillance would require.[197]

VI. CONCLUSION

In light of predictive analytics' significant role in people's lives, it seems inevitable that the government will eventually turn to predictive surveillance. Assuming that the government can overcome the technical and political challenges, predictive surveillance will present a significant doctrinal challenge. Courts will feel great pressure to approve predictive surveillance, and they will have a variety of doctrinal approaches at their disposal. This Article proposes that courts should adopt the narrowest possible approach to avoid destabilizing existing Fourth Amendment doctrine. The narrowest approach would be to avoid dramatic expansion of the third-party and public-exposure doctrines, and rely instead on the *Keith* case's domestic security exception to the warrant requirement. Not only would that approach avoid creating or expanding an exception to the warrant requirement; it would also limit the use of predictive surveillance to domestic security threats. Such an approach would represent a reasonable compromise between the promise of predictive surveillance and the intrusion posed by bulk data collection.

---

[197] For a discussion of the safeguards that Congress would need to build into a predictive surveillance statute, see, Spencer, *supra* note 10, at 527-36.